



22883

PATENT TRADEMARK OFFICE

## PATENT APPLICATION

This application is submitted in the name of the following inventors:

<i>Inventor</i>	<i>Citizenship</i>	<i>Residence City and State</i>
Michael MALCOLM	United States	Aspen, CO
Daniel COLLENS	Canada	Waterloo, Ontario (Canada)
Stephen WATSON	Canada	Toronto, Ontario (Canada)
Paul RECHSTEINER	Canada	Toronto, Ontario (Canada)
Kevin HUI	Canada	Toronto, Ontario (Canada)

The assignee is *Kaleidescape*, a corporation having an address in Mountain View, California.

## TITLE OF THE INVENTION

Secure Presentation Of Media Streams in Response to Encrypted Digital Content

## BACKGROUND OF THE INVENTION

### 1. *Field of the Invention*

The invention relates to presentation of media streams in response to digital content.

### 2. *Related Art*

Distribution of digital content representing media streams, such as for example movies, is subject to several problems. One problem is that it is easy to make exact copies of digital content, thus allowing any recipient of that content to redistribute it, whether authorized or not. It would be advantageous to be able to distribute digital content, particularly digital content representing media streams, without fear of its unauthorized distribution. This would be particularly advantageous when it is desired to distribute digital content using a communication link, such as for example a computer network or other technique for distribution to end viewers (for example, either on demand, in anticipation of future demand, or in response to something else).

One known solution is to encrypt the digital content that represents the media stream, so that a recipient of that digital content cannot easily redistribute it in a readily presentable (that is, unencrypted) format to unauthorized recipients. However,

1 even when digital content is distributed in an encrypted form, it must be decrypted be-  
2 fore it can be presented to a viewer. Thus, there is at least some time for each movie,  
3 during distribution from originator to viewer, during which that movie is available in  
4 an unencrypted format (herein sometimes also called "in the clear"). At times, and in  
5 places in any presentation system, when that movie is available in the clear, that movie  
6 is vulnerable to security attacks. For example, an unauthorized person might copy the  
7 movie in its unencrypted format and distribute or use it without authorization.

8  
9 Accordingly, it would be advantageous to provide a method (and devices  
10 for performing it) by which the digital content can be used for presentation as a media  
11 stream, without exposing that digital content in the clear. However, there are several  
12 issues related to achieving this goal.

- 13
- 14 • It would be desirable for the device to be relatively tamper-resistant, so that the  
15 work factor for obtaining the digital content in the clear would be substantially  
16 greater than simply purchasing copies (or at least, greater than other possibly  
17 available techniques for unauthorized procurement).
  - 18
  - 19 • It would also be desirable for the device to expose the digital content represent-  
20 ing the media stream as little as possible. For some examples, having the digital  
21 content (or a key from which that digital content could be obtained) in the clear  
22 in a memory would be less desirable than only having the digital content in the

1 clear on an internal bus, which itself would be less desirable than only having the  
2 digital content in the clear when actually presented on a screen for viewing by an  
3 end-user.  
4

5 These issues present a need for separating that part of the device that has  
6 access to keys for decryption into a separate set of "trusted" hardware and software  
7 elements, with the effect that it would be advantageous for at least some of the device to  
8 be implemented in tamper-resistant hardware operating under control of verified soft-  
9 ware.  
10

- 11 • It would be desirable for the device to be able to both decode digital content rep-  
12 resenting media streams, and to provide common playback functions known for  
13 media streams, without these functions involving complete decryption of the  
14 digital content. These functions might include navigation within the digital  
15 content (such as for example fast-forward and rewind functions), content selec-  
16 tion within the digital content (such as for example chapter-skip and multi-angle  
17 selection functions), or manipulation of the presentation (such as for example  
18 freeze-frame or single-frame-advance functions).  
19

- 20 • It would be desirable for the device to be able to provide access to metadata  
21 about the one or more media streams, such as a title or rating, or other informa-  
22 tion about the media streams for which it is generally acceptable to maintain that

1 information in the clear, without these functions involving complete decryption  
2 of the digital content.

- 3
- 4 • It would be desirable for the device to be able to provide differing access to dis-  
5 tinct end-users for selected portions of one or more media streams, such as for  
6 example differing access to audio versus video, or English-language versus  
7 French-language versions, or US releases versus UK releases, or "airline" ver-  
8 sions versus "general release" versions, for the same media stream, without these  
9 functions involving complete decryption of the digital content.
- 10

11 It would be desirable for these playback functions, and possibly others, to  
12 be implemented in relatively unverified software. In one embodiment, only verified  
13 hardware or software would be allowed access to keys for decrypting the digital con-  
14 tent. However, there are many such functions for which it would be desirable to have  
15 them be available to the user, without having those functions be implemented in tam-  
16 per-resistant hardware (which would be more expensive, and would be difficult to up-  
17 date), or in verified software (which would also be more difficult to update, and might  
18 also be more expensive to create).

19

20 Formats now used for encoding digital content representing a media  
21 stream for digital distribution (such as for example MPEG-1, MPEG-2, and MPEG-4) are  
22 relatively complex. These formats provide for dividing up the digital content into mul-

1 tiple packets. Thus, it is possible when parsing digital content representative of media  
2 streams, that encryption might involve maintaining substantial state information across  
3 many such packets. A device able to conduct both the parsing and stitching operations  
4 might need substantial working memory. In general, having to maintain less state  
5 across packet boundaries would allow the hardware and software for decoding and de-  
6 crypting the encoded and encrypted movie to be simpler, and would allow the digital  
7 content for the movie to be less exposed in the clear.

8  
9           Formats used for encoding digital content representing media streams  
10 also provide for partial delivery of portions of the digital content at different times, such  
11 as when sending the digital content is interrupted and later restarted, or when packets  
12 including portions of the digital content arrive out of order, or with parts missing.  
13 Similar to the problem involving multiple packets, a device able to recover from partial  
14 delivery of only a portion of the digital content might need to maintain substantial state,  
15 or to maintain substantial working memory. In general, having to maintain less state  
16 across packet boundaries would allow the hardware and software for decoding and de-  
17 crypting the encoded and encrypted movie to be more robust with regard to handling  
18 packets that arrive out of order, or with parts missing.

19  
20           Formats used for encoding digital content representing media streams  
21 provide for additional information about the media stream, such as a title, for which it  
22 might be advantageous to have available even when the media stream is not actually

1 being presented to the viewer. For example, it might be advantageous to allow a po-  
2 tential viewer to browse titles and related information, or even to conduct a computer-  
3 ized search on that information, without actually presenting the media stream. A de-  
4 vice able to provide that information rapidly, such as on a random access basis with re-  
5 gard to the digital content representing that media stream, would involve substantial  
6 resources for computation and memory, likely relatively proportionate to the amount of  
7 the digital content desired to be reviewed on a random access basis, with the effect that  
8 such a device would thus be relatively insecure against attack, as either decryption keys  
9 or digital content in the clear would be available to those parts of the system for which  
10 such random access were desired.

11  
12 Accordingly, it would be advantageous to provide an improved technique  
13 for presentation of digital content representing a media stream, such as the technique in  
14 which devices able to access the digital content are not allowed access to the media  
15 stream represented by that digital content, but still are allowed access to metadata re-  
16 garding that media stream.

## 17 18 SUMMARY OF THE INVENTION

19  
20 A method of secure presentation of media streams in response to en-  
21 crypted digital content includes (1) encoding the media stream into a digital content  
22 format representing that media stream, (2) encrypting a portion of that digital content,

1 less than the entire digital content format representing that media stream, the portion of  
2 the digital content that is encrypted being required for presentation of the media  
3 stream, (3) in which the encrypted version of the digital content is substantially un-  
4 changed in formatting parameters from the clear version of the digital content.

5  
6           Formats used for encoding digital content representing media streams  
7 provide for encapsulating information in a hierarchy of layers, each relatively higher-  
8 level layer representing an abstraction for which each relatively lower-level layer repre-  
9 sents an implementation thereof. As described herein, in an aspect of the invention, the  
10 highest-level layer (or multiple higher-level layers) represent audio and video informa-  
11 tion for the media stream, while relatively lower-level layers represent techniques by  
12 which that information is broken into packets, indexed, multiplexed, and supplemented  
13 with metadata (such as for example closed captioning and copyright information). As  
14 described herein, in an aspect of the invention, only the audio and video information for  
15 the media stream is encrypted, while other relatively lower-level layers remain "in the  
16 clear" (that is, unencrypted).

17  
18           More generally, formats used for encoding digital content representing  
19 media streams provide a tree-structure in which information is disposed, the audio and  
20 video data being incorporated into leaves of the tree and various types of metadata  
21 (such as for example control information) being incorporated into branches of the tree.  
22 After reading this application, those skilled in the art will recognize that a tree structure



1 is not the only possible format, and that in general, any partial ordering of information  
2 might be specified by a format used for encoding digital content representing media  
3 streams, where the audio or video data are specified to have a selected ordering with  
4 regard to metadata for that digital content.

5  
6 As described herein, in an aspect of the invention, where that format used  
7 for encoding the digital content can be represented as a tree, it suffices for a subtree of  
8 the digital content closed root-ward to be unencrypted. In this context, "closed root-  
9 ward" describes the case where if a node X in the tree T is included in a set of nodes  
10 (and thus unencrypted), so is every node in a path from X toward the root of the tree T.  
11 In one embodiment, substantially all the leaves of the tree T are encrypted, and the sys-  
12 tem is still able to parse the MPEG stream, with the only limitation being that the sys-  
13 tem cannot present the actual audio or video without decryption of those leaves.

14  
15 Similarly, where that format used for encoding the digital content can be  
16 represented as a partial ordering, it suffices for a portion of that partial ordering closed  
17 backward under that partial ordering to be unencrypted. In this context, "closed  
18 backward" describes the case where if an element X in the partial ordering P is included  
19 in a set of elements (and thus unencrypted), so is every element Y for which  $Y < X$  in the  
20 partial ordering P. In one embodiment, substantially all the audio and video elements  
21 of the partial ordering P are encrypted, and the system is still able to parse the MPEG

1 stream, with the only limitation being that the system cannot present the actual audio or  
2 video without decryption of those audio and video elements.

3  
4 More generally, in this context "encrypted" and "unencrypted" can be re-  
5 placed with distinct levels of hardness to decode the associated elements X and Y with-  
6 out having a presentation device key. For one example, not intended to be limiting in  
7 any way, the audio and video elements of the tree T (or the partial ordering P) might be  
8 encrypted using the AES-128 block cipher, while the control elements, MPEG packet  
9 headers, and MPEG pack headers might be encrypted using a substantially less secure  
10 technique, such as a bitwise XOR with a selected password. As described above, so  
11 long as the less-strongly encrypted portions form a collection that is closed root-ward  
12 (for a tree T) or closed backward (for a partial ordering P), the system will be able to  
13 parse the MPEG stream in relatively non-secure hardware and software, while still be-  
14 ing limited to a relatively secure portion with the appropriate key to present audio and  
15 video.

16  
17 After reading this application, those skilled in the art will recognize that  
18 more generally, "encryption" can be replaced by any security technique, such as for ex-  
19 ample physical hardware security such as hidden mask layers in a ROM or ASIC. For  
20 one example, multiple levels of security might include (a) a first level readable like a file  
21 in a computer; (b) a second level readable only by coupling a probe to an external port  
22 of the presentation device, (c) a third level readable only by coupling a probe to an in-

1 ternal bus of the presentation device, (d) a fourth level readable only by emulation of  
2 the circuitry of the presentation device, and (e) a fifth level readable only by reverse en-  
3 gineering of the integrated circuit and examination with an electron microscope.

4  
5           An aspect of the method includes selecting those portions of the digital  
6 content for encryption so that there is no substantial change in distribution of the digital  
7 content representing the media stream, such as for example (1) packetization of the  
8 digital data, or (2) synchronization of audio with video portions of the media stream. In  
9 a preferred embodiment, unchanged distribution can be accomplished by making no  
10 substantial change in length of portions of the video packet data, such as for example  
11 individual packets of an MPEG-encoded movie.

12  
13           In one embodiment, the method includes, when encoding the media  
14 stream into a digital content format, such as for example MPEG-2, (1) refraining from  
15 encrypting information by which the video packet data is described, such as for exam-  
16 ple packet formatting information, and (2) encrypting the video packet data using a  
17 block-substitution cipher. For example, a block-substitution cipher can be used to en-  
18 crypt each sequence of 16 bytes of video data in each packet, possibly leaving as many  
19 as 15 bytes of video data in each packet in the clear. In one embodiment, the method  
20 includes (3) separately encrypting the audio portion of the media streams, and possibly  
21 other selected data portions of the media streams, within the digital content, with the ef-

fect that these separate data portions of the media streams might be made differently available to distinct selected users or groups of users.

The invention is not restricted to movies, but is also applicable to other media streams, such as for example animation or sound, as well as to still media, such as for example pictures or illustrations, and to databases and other collections of information.

#### BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 shows a block diagram of a system for secure presentation of media streams in response to encrypted digital content.

Figure 2 shows a process flow diagram of a method for secure presentation of media streams in response to encrypted digital content.

#### INCORPORATED DISCLOSURE

This application claims priority of the following documents, each of which is hereby incorporated by reference as if fully set forth herein.

- 1       • U.S. provisional patent application 60/394,630, filed July 9, 2002, in the name of  
2       Michael Malcolm, Stephen Watson, Daniel Collens, and Kevin Hui, attorney  
3       docket number 217.1001.01, titled "Watermarking and Fingerprinting a Movie  
4       for Secure Distribution."  
5
- 6       • U.S. provisional patent application 60/394,922, filed July 9, 2002, in the name of  
7       Michael Malcolm, Stephen Watson, and Daniel Collens, attorney docket number  
8       217.1002.01, titled "System Architecture of a System for Secure Distribution of  
9       Media."  
10
- 11      • U.S. provisional patent application 60/394,588, filed July 9, 2002, in the name of  
12      Michael Malcolm, Stephen Watson, and Daniel Collens, attorney docket number  
13      217.1003.01, titled "Topology of Caching Nodes in a System for Secure Delivery  
14      of Media Content."  
15
- 16      • U.S. patent application 10/356,692, filed January 31, 2003, in the name of Daniel  
17      Collens, Stephen Watson, and Michael Malcolm, attorney docket number  
18      217.1004.01, titled "Parallel Distribution and Fingerprinting of Digital Content".  
19
- 20      • U.S. patent application 10/356,322, filed January 31, 2003, in the name of Stephen  
21      Watson, Daniel Collens, and Kevin Hui, attorney docket number 217.1005.01, ti-

1       tled "Watermarking and Fingerprinting Digital Content Using Alternative Blocks  
2       to Embed Information".

- 3
- 4       • U.S. patent application 10/377,266, filed February 28, 2003, in the name of Ste-  
5       phen WATSON, attorney docket number 217.1006.01, titled "Recovering from  
6       De-Synchronization Attacks Against Watermarking and Fingerprinting".
  - 7
  - 8       • U.S. patent application 10/378,046, filed February 28, 2003, in the name of Ste-  
9       phen WATSON, attorney docket number 217.1007.01, titled "Detecting Collusion  
10       Among Multiple Recipients of Fingerprinted Information".
  - 11
  - 12       • U.S. patent application 10/\_\_\_\_\_, filed this same day, in the name of Stephen  
13       WATSON, Michael MALCOLM, and Daniel COLLENS, attorney docket number  
14       217.1010.01, titled "Content and Key Distribution System for Digital Content  
15       Representing Media Streams".
- 16

17               These documents are hereby incorporated by reference as if fully set forth  
18       herein, and are sometimes referred to herein as the "incorporated disclosure".

19

20               Inventions described herein can be used in combination or conjunction  
21       with technology described in the incorporated disclosure.

22

## 1 DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

2  
3 In the description herein, a preferred embodiment of the invention is de-  
4 scribed, including preferred process steps and data structures. Those skilled in the art  
5 would realize, after perusal of this application, that embodiments of the invention  
6 might be implemented using a variety of other techniques not specifically described,  
7 without undue experimentation or further invention, and that such other techniques  
8 would be within the scope and spirit of the invention.

9  
10 *Lexicography*

11  
12 The general meaning of each of these following terms is intended to be il-  
13 lustrative and in no way limiting.

- 14  
15 • The phrase "media stream" describes information intended for presentation in a  
16 sequence, such as motion pictures including a sequence of frames or fields, or  
17 such as audio including a sequence of sounds. As used herein, the phrase  
18 "media stream" has a broader meaning than the standard meaning for  
19 "streaming media," (of sound and pictures that are transmitted continuously  
20 using packets and that start to play before all of the content arrives). Rather, as  
21 described herein, there is no particular requirement that "media streams" must  
22 be delivered continuously. Also as described herein, media streams can refer to

1 other information for presentation, such as for example animation or sound, as  
2 well as to still media, such as for example pictures or illustrations, and also to  
3 databases and other collections of information.

- 4  
5 • The phrase “digital content” describes data in a digital format, intended to repre-  
6 sent media streams or other information for presentation to an end viewer.  
7 “Digital content” is distinguished from packaging information, such as for ex-  
8 ample message header information. For the two phrases “digital content” and  
9 “media stream,” the former describes a selected encoding of the latter, while the  
10 latter describes a result of presenting any encoding thereof.

- 11  
12 • The phrase “embedded information in a media stream” describes information in-  
13 corporated into a set of digital content representing that media stream, in a form  
14 capable of later detection. For example, digital content representing media  
15 streams might include embedded information, such that the media streams are  
16 still capable of presentation to a viewer without substantial change, but in which  
17 the embedded information can be recovered by suitable processing of the digital  
18 content.

- 19  
20 • The phrase “embedding information in a media stream” describes generating a  
21 set of digital content representing that media stream, for which the digital con-



1       tent both represents the media stream and also includes the embedded informa-  
2       tion in a form capable of later detection.

- 3
- 4       • The term “watermark” describes a schema for digital content by which  
5       information can be embedded into that digital content. In preferred  
6       embodiments, as described in related applications, an attacker cannot easily  
7       remove the watermark. However, the concept of a watermark as described  
8       herein is sufficiently general to include watermarks that are not so resistant to  
9       attack, or which use other techniques for embedding information.

- 10
- 11       • The term “fingerprint” and the phrase “embedded identifying information”  
12       describe sets of information sufficient to identify at least one designated recipient  
13       of digital content. In a preferred embodiment, as described in a related applica-  
14       tion, multiple attackers colluding together cannot easily remove the fingerprint  
15       provided by the invention, or prevent at least one of them from being detected as  
16       unauthorized distributor of the digital content. However, the concept of the  
17       fingerprint as described herein is sufficiently general to include fingerprints that  
18       are not so resistant to removal, or do not provide such capability for detecting  
19       unauthorized distributors of the digital content, or which use other techniques  
20       for embedding information, for detecting the embedded information, or for de-  
21       tecting unauthorized distributors of the digital content.

1 As described in the incorporated disclosure and in related applications, a “wa-  
2 termark” refers to a set of locations in a media stream at which information  
3 might be embedded, while a “fingerprint” refers to the actual information that is  
4 embedded, such as for example by selecting a block or alt-block for each such lo-  
5 cation. However, in the context of the invention, there is no requirement that the  
6 concepts of watermarking and fingerprinting be so restricted. More generally, a  
7 watermark might be used for any technique by which a source of the digital  
8 content for the media stream might be identified, or a fingerprint might be used  
9 for any technique by which a recipient of the digital content for the media stream  
10 might be identified. For example, not intended to be limiting in any way, wa-  
11 termarking and fingerprinting information as described herein includes a repre-  
12 sentation of the entire path (or set of paths) by which the digital content repre-  
13 senting the media stream was sent from its source and received by its end viewer  
14 (or equipment associated therewith).

- 15  
16 • The phrase “identifying information” describes, generally, either information  
17 associated with a watermark, information associated with a fingerprint, or other  
18 information by which authorized or unauthorized distribution of digital content  
19 representing a media stream might be identified.

- 20  
21 • The phrases “original movie” and “alt-movie” describe alternative versions of  
22 the same media stream, such as one being an original version of that media

1 stream introduced into a system using aspects of the invention, and another  
2 being an alternative version of that same media stream generated in response to  
3 the original movie. Similarly, the phrases "original block" and "alt-block"  
4 describe alternative versions of the same individual block or macroblock within  
5 the original movie or alt-movie. As described in a related application, a  
6 difference between the original movie and the alt-movie is historical, in that the  
7 alt-movie can be substituted for the original movie in nearly every respect.  
8 Similarly, a difference between any one original block and its associated alt-block  
9 is historical, in that the alt-block can be substituted for the original block in  
10 nearly every respect.

- 11
- 12 • The phrases "original digital content" and "altered digital content" (or in the  
13 latter case, "post-attack digital content") describe digital content representing  
14 media streams, in a first format (original digital content) and in a second format  
15 (altered digital content), the altered digital content having been produced in re-  
16 sponse to the original digital content and with the intent of representing sub-  
17 stantially similar media streams, but with the effect that detecting identifying in-  
18 formation from the original digital content is made relatively difficult. Thus, the  
19 altered digital content is a result of a de-synchronization attack on the original  
20 digital content. In preferred embodiments, the original digital content might be  
21 an actual original of some digital content before it was subject to a de-  
22 synchronization attack, or might be a constructed form of digital content, such as

1 in response to an original movie and alt-movie, or in response to a set of original  
2 blocks and alt-blocks. For one example, not intended to be limiting in any way,  
3 the original digital content might be an average of the original movie and the alt-  
4 movie, or there might be two sets of original digital content, one for the original  
5 movie and one for the alt-movie. In one embodiment, a typical case of original  
6 digital content will include a block-by-block selection from the blocks of the  
7 original movie and the alt-movie. However, in the context of the invention, there  
8 is no particular restriction to such formats being used or included as the "original  
9 digital content" for which resynchronization is sought. Moreover, as described  
10 below, numerous variations on this theme are all within the scope and spirit of  
11 the invention, and would be workable without undue experimentation or further  
12 invention.

- 13
- 14 • The phrase "end viewer" describes a recipient of the media stream for whom de-  
15 coding of the digital content representing the media stream, and presentation of  
16 the media stream, is contemplated.

- 17
- 18 • The term "decoding" describes generating data in a form for presentation of the  
19 media stream, in response to the digital content representing the media stream in  
20 an encoded format. As described herein, the encoded format might include an  
21 industry standard encoded format such as MPEG-2. However, the concept of

1 decoding as described herein is sufficiently general to include other encoding  
2 formats for media streams.

- 3
- 4 • The term "presentation" describes generating information in a form for viewing  
5 of the media stream, such as for example audio and visual information for  
6 viewing a movie. As described herein, presentation of a movie might include  
7 visual display of the frames or fields of motion picture, as well as audio presen-  
8 tation of a soundtrack associated with that motion picture. However, the con-  
9 cept of presentation as described herein is sufficiently general to include a wide  
10 variety of other forms of generating information for viewing.

- 11
- 12 • The term "packet" describes a portion of the digital content representing a media  
13 stream, such as for example as might be separately identifiable within that digital  
14 content 111 or transmitted when sending that digital content. In one embodi-  
15 ment, a "packet" indicates a contiguous sub-region of an MPEG-2 packet in-  
16 cluding picture slice data. In the context of the invention, a "packet" is not nec-  
17 essarily the same as an MPEG-2 packet, and a "packet" is not necessarily the  
18 same as a TCP/IP packet.

19

20 Other and further applications of the invention, including extensions of  
21 these terms and concepts, would be clear to those of ordinary skill in the art after pur-  
22 chasing this application. These other and further applications are part of the scope and

1 spirit of the invention, and would be clear to those of ordinary skill in the art without  
2 further invention or undue experimentation.

3  
4 The scope and spirit of the invention is not limited to any of these defini-  
5 tions, or to specific examples mentioned therein, but is intended to include the most  
6 general concepts embodied by these and other terms.

7  
8 *System Elements*

9  
10 Figure 1 shows a block diagram of a system for secure presentation of  
11 media streams in response to encrypted digital content.

12  
13 A system 100 includes a media stream source 110, a distribution network  
14 120, a key server 130, and a set of customer premises equipment 140. The system 100 is  
15 disposed for presenting one more media streams, as represented by digital content as-  
16 sociated with those media streams, to one or more particular selected users 150.

17  
18 The media stream source 110 is capable of injecting a set of digital content  
19 111, in the form of a sequence of packets 112, the sequence of packets 112 including  
20 digital content for at least one media stream intended for a user 150 of the system 100.  
21 In one embodiment, there might be more than one media stream source 110, and the

1 media stream sources 110 are capable of injecting copies of the digital content adapted  
2 to particular selected users 150.

3  
4 The distribution network 120 is disposed for transferring information  
5 between and among the media stream source 110, the key server 130, and the customer  
6 premises equipment 140. In one embodiment, the distribution network 120 includes a  
7 set of intermediate caches or sources 121, capable of receiving packets 112 from the me-  
8 dia stream sources 110, caching or otherwise maintaining in storage information from  
9 those packets 112, and further adapting the digital content associated with those pack-  
10 ets 112 to particular selected users 150.

11  
12 Those skilled in the art will recognize, after perusal of this application,  
13 that the system 100, including the media stream source 110, the distribution network  
14 120, and the intermediate caches or sources 121, are preferably disposed for adapting  
15 and encrypting the digital content 111 (as further described with regard to distribution  
16 of digital content representing media streams) as described in the incorporated disclo-  
17 sure, such as for example in the documents "Watermarking and Fingerprinting a Movie  
18 for Secure Distribution," "System Architecture of a System for Secure Distribution of  
19 Media," "Topology of Caching Nodes in a System for Secure Delivery of Media Con-  
20 tent," "Parallel Distribution and Fingerprinting of Digital Content," and "Watermark-  
21 ing and Fingerprinting Digital Content Using Alternative Blocks to Embed Informa-  
22 tion."

1  
2           As further described herein, in one embodiment, not intended to be lim-  
3 iting in any way, the digital content 111 is encoded using an MPEG-2 encoding scheme,  
4 with selected portions of that digital content 111, representative of the media stream,  
5 encrypted as described in the incorporated disclosure, such as for example in the  
6 documents "Watermarking and Fingerprinting a Movie for Secure Distribution," "Sys-  
7 tem Architecture of a System for Secure Distribution of Media," "Topology of Caching  
8 Nodes in a System for Secure Delivery of Media Content," "Parallel Distribution and  
9 Fingerprinting of Digital Content," and "Watermarking and Fingerprinting Digital  
10 Content Using Alternative Blocks to Embed Information." The selected portions of that  
11 digital content 111 preferably include only the portions of the digital content 111 repre-  
12 sentative of the presentable or displayable portions of the media stream, and preferably  
13 do not include any formatting data, metadata, or other descriptive data relating to the  
14 media stream, even if embedded in the encoded digital content 111 representative of  
15 that media stream.

16  
17           As further described herein, in one embodiment, not intended to be lim-  
18 iting in any way, those portions of the digital content 111 are encoded with the effect  
19 that the sequence of packets 112 is substantially unchanged from an alternative se-  
20 quence of packets 112 that might have been generated for the digital content 111, had  
21 that digital content 111 not been encrypted for distribution to the user 150. For exam-  
22 ple, this has the effect that the length of each packet 112 in the sequence of packets 112 is



1 substantially unchanged from an alternative sequence of packets 112 that might have  
2 been generated for the digital content 111 had that digital content 111 not been en-  
3 crypted for distribution to the user 150. This has the effect that the amount of interme-  
4 diate state maintained for decoding that sequence of packets 112, and thus for decoding  
5 that digital content 111, is substantially unchanged from an alternative sequence of  
6 packets 112 that might have been generated for the digital content 111, had that digital  
7 content 111 not been encrypted for distribution to the user 150.

8  
9 As further described herein, in one embodiment, not intended to be lim-  
10 iting in any way, those portions of the digital content 111 are encoded with the effect  
11 that synchronization of audio with video within the digital content 111 is substantially  
12 unchanged from an alternative operation of synchronization of audio with video within  
13 the digital content 111 that might have been performed for that digital content 111, had  
14 that digital content 111 not been encrypted for distribution to the user 150. This has the  
15 effect that the degree of effort involved in decoding that digital content 111, any de-  
16 coding steps involving synchronization of audio with video, are relatively equivalent to  
17 the degree of effort involved in an operation of synchronization of audio with video  
18 within the digital content 111 that might have been generated for the digital content  
19 111, had that digital content 111 not been encrypted for distribution to the user 150.

20  
21 As further described herein, in one embodiment, not intended to be lim-  
22 iting in any way, those portions of the digital content 111 are encoded with the effect

1 that locating (or "seeking to") a selected position in a position in the media stream rep-  
2 resented by the digital content 111 is substantially unchanged from an alternative op-  
3 eration of locating (or "seeking to") a selected position in a position in the media stream  
4 represented by the digital content 111 that might have been performed for that digital  
5 content 111, had that digital content 111 not been encrypted for distribution to the user  
6 150. This has the effect that the degree of effort involved in an operation of locating (or  
7 "seeking to") a selected position in a position in the media stream represented by the  
8 digital content 111 is substantially unchanged from an alternative operation of locating  
9 (or "seeking to") a selected position in a position in the media stream represented by the  
10 digital content 111 that might have been performed for that digital content 111, had that  
11 digital content 111 not been encrypted for distribution to the user 150.

12  
13 Moreover, as further described herein, in one embodiment, not intended  
14 to be limiting in any way, in the context of the invention, it is not necessary to decrypt  
15 portions of the digital content 111 to perform an operation of locating (or "seeking to") a  
16 selected position in a position in the media stream represented by the digital content  
17 111. After reading this application, those skilled in the art would recognize that the op-  
18 eration of locating (or "seeking to") a selected position in a position in the media stream  
19 represented by the digital content 111 might thus be performed relatively more effi-  
20 ciently (that is, without substantial additional encryption steps) and relatively more se-  
21 curely (that is, by relatively less trusted hardware or software components). In one em-  
22 bodiment, those portions of the digital content 111, in an MPEG-2 encoding of that

1 digital content 111, useful for that operation of locating (or "seeking to") a selected po-  
2 sition in a position in the media stream are not encrypted.

3  
4 As further described herein, in one embodiment, not intended to be lim-  
5 iting in any way, within the digital content 111, only the video block data is encrypted,  
6 preferably using a block-substitution cipher, preferably a variation of the AES cipher,  
7 such as for example AES-128 or AES-256. In one embodiment, the block-substitution  
8 cipher can be used to encrypt each sequence of 16 bytes of video block data in each  
9 packet 112, with the fact that as many as 15 bytes of video block data within each packet  
10 112 might remain in the clear after encryption.

11  
12 In one embodiment, the digital content 111 is encoded using MPEG-2,  
13 which includes its audio and video data (as well as control data) within an MPEG  
14 "packet." MPEG packets are enclosed by MPEG-2 within an MPEG "pack." The MPEG  
15 standard is further described in documents known in the digital video industry. This  
16 has the effect that, in such embodiments, only audio or video data is encrypted (but not  
17 necessarily all audio and video data is encrypted), while substantially all of the MPEG  
18 control data (including MPEG packet headers, MPEG pack headers, and in general all  
19 types of MPEG control data), is left unencrypted. This also has the effect that, in such  
20 embodiments, only MPEG packet payloads are encrypted.

1           In such embodiments, where an MPEG packet includes a payload that is  
2 not an integer multiple of the encryption size (16 bytes), any remainder, possibly as  
3 many as 15 bytes, is also left unencrypted. This has the effect that, in such embodi-  
4 ments, at least some packets 112 might include packet header information (unen-  
5 crypted), MPEG control data (unencrypted), audio or video data that is encrypted, and  
6 possibly as many as 15 bytes of audio or video data that is left unencrypted.

7  
8           In such embodiments, where the MPEG data has already been encrypted  
9 with another technique (such as for example CSS, which might be in use for selected  
10 DVD physical media carrying the MPEG data), those packets 112 already encrypted  
11 with the other technique are not further encrypted using the AES cipher. Those skilled  
12 in the art will recognize that because the CSS specification provides that no more than  
13 50% of sectors of a DVD video disk are encrypted using CSS, this has the effect that as  
14 many as 50% of sectors of the DVD video disk would remain to be possibly encrypted  
15 using the AES cipher.

16  
17           In such embodiments, those data elements of the MPEG packet that have  
18 been encrypted are maintained as offsets into the MPEG pack information and MPEG  
19 packet information. This has the effect that, although the MPEG pack information and  
20 MPEG packet information have variable-length headers, the encrypted data elements  
21 can still be located relative to the end of those headers.

1           As further described herein, in one embodiment, not intended to be lim-  
2    iting in any way, within the digital content 111, separable media streams, such as for  
3    example an audio stream distinguishable from the video stream, are preferably sepa-  
4    rately encrypted, with the effect that the separable media streams might be made differ-  
5    ently available to distinct particular selected users 150, or distinct groups of particular  
6    selected users 150.

7  
8           The key server 130 is capable of supplying, such as for example in re-  
9    sponse to a request from the user 150, digital information including decryption keys  
10   (whether symmetric keys, or asymmetric keys such as used in public key cryptosys-  
11   tems) and license information to particular selected users 150.

12  
13          The customer premises equipment 140 includes a local library 141, a local  
14   area network 142, and a set of player equipment 143. The customer premises equip-  
15   ment 140 is disposed for presenting one or more media streams, as represented by  
16   digital content included in the sequence of packets 112, to one or more particular se-  
17   lected users 150 associated with the particular selected customer premises equipment  
18   140.

19  
20          The local library 141 includes a processor 141a, program and data memory  
21   or mass storage 141b, and a formatted-media reader 141c. In one embodiment, the local  
22   library 141 also includes at least one input element 141d and at least one output element

1 141e. The memory or mass storage 141b is capable of including instructions 141f capa-  
2 ble of being executed or interpreted by the processor 141a to perform steps as described  
3 herein. The memory or mass storage 141b is also capable of maintaining copies of at  
4 least portions of the digital content 111, possibly watermarked or fingerprinted as de-  
5 scribed in the incorporated disclosure.

6  
7 As described below, the instructions 141f direct the local library 141 to  
8 perform the following actions:

9  
10 (A1a) to receive digital content 111 from the media stream source 110, using the  
11 format of the sequence of packets 112, or

12  
13 (A1b) to receive digital content 111 from the formatted-media reader 141c;

14  
15 In the event that the digital content 111 is received from the formatted-  
16 media reader 141c, that digital content 111 might either be (1) already encrypted on the  
17 physical media being read by the device, (2) unencrypted on the physical media being  
18 read by the device, or (3) encrypted on the physical media being read by the device, but  
19 using a non-preferred encryption technique. In case 2, the digital content 111 is en-  
20 crypted by the formatted-media reader 141c, or by an supplemental device coupled  
21 thereto, before transferring any digital content 111 to devices other than the formatted-  
22 media reader 141c. In case 3, the digital content 111 is decrypted using the non-

1 preferred encryption technique, and re-encrypted using a preferred encryption tech-  
2 nique, before transferring any digital content 111 to devices other than the formatted-  
3 media reader 141c.

4 (A2) (optionally) to partially decode that digital content 111, with the effect of  
5 retrieving at least some metadata regarding that digital content 111 in the clear,  
6 such as for example index files including pointers into the digital content 111;  
7

8 (A3) to maintain that encrypted digital content 111, and optionally at least some  
9 decrypted metadata regarding that digital content 111, in the memory or mass  
10 storage 141b; and  
11

12 (A4) to decode that digital content 111, with the effect of retrieving metadata re-  
13 garding that digital content 111 in the clear, and with the effect of retrieving data  
14 representing presentable portions of the media stream represented by that digital  
15 content 111 in an encrypted form;  
16

17 (A5) to transfer that encrypted digital content 111 from the memory or mass  
18 storage 141b to the local network 142 and to the player equipment 143; and  
19

20 (A6) to decrypt selected portions of that digital content 111, in response to re-  
21 quests from the player equipment 143, with the effect of retrieving, in the clear

1 but secure from detection or intrusion, data represented by that digital content  
2 111 for presenting a media stream at the player equipment 143.

3  
4 The specific techniques to be applied are further described below.

5  
6 As described below, the player equipment 143 performs the following ac-  
7 tions:

8  
9 (B1) receives the decoded digital content 111 from the memory or mass storage  
10 141b and the local network 142;

11  
12 (B2) receives a set of commands or requests from the user 150;

13  
14 (B3) performs those commands or requests from the user 150 capable of being  
15 performed without reference to encrypted elements of the decoded digital con-  
16 tent 111, without performing any decryption on that decoded digital content 111;  
17 and

18  
19 (B4) presents or displays those elements of the decoded digital content 111 that  
20 involve decrypting elements (such as audio or video blocks) of that decoded  
21 digital content 111, using one or more decryption keys from the key server 130.



1 The specific techniques to be applied are further described below.

2  
3 *Method of Operation*  
4

5 Figure 2 shows a process flow diagram of a method for secure presenta-  
6 tion of media streams in response to encrypted digital content.  
7

8 Although described serially, the flow points and method steps of the  
9 method 200 can be performed by separate elements in conjunction or in parallel,  
10 whether asynchronously or synchronously, in a pipelined manner, or otherwise. In the  
11 context of the invention, there is no particular requirement that the method must be  
12 performed in the same order in which this description lists flow points or method steps,  
13 except where explicitly so stated.  
14

15 At a flow point 210, the local library 141 is ready to receive digital content  
16 111 representing one or more media streams. The method 200 performs either the step  
17 211 (receiving digital content 111 from the media stream source 110), or the step 212 (re-  
18 ceiving digital content 111 from the formatted-media reader 141c).  
19

20 At a step 211, the local library 141 receives digital content 111 representing  
21 one or more media streams from the media stream source 110. As part of this step, the  
22 local library 141 receives a sequence of one or more packets 112, collectively including

1 the digital content 111. As part of this step, the local library 141 might be required to  
2 request retransmission of lost or broken packets 112, might be required to reorder pack-  
3 ets 112 delivered out of sequence, and might be required to re-establish a connection  
4 with the media stream source 110 to continue receiving from a known breakpoint. As a  
5 result of this step, the local library 141 obtains at least a portion of the digital content  
6 111 representing one or more media streams, and the method 200 is able to proceed at  
7 the flow point 220.

8  
9 At a step 212, the local library 141 receives digital content 111 representing  
10 one or more media streams from the formatted-media reader 141c. As part of this step,  
11 the local library 141 receives data directly from the formatted-media reader 141c or  
12 from a supplemental device coupled thereto. That data might be delivered in a se-  
13 quence of one or more packets 112, in a similar manner to performance of the step 211,  
14 or might be delivered by another technique, such as for example a DMA transfer. As  
15 noted above, that digital content 111 might either be already encrypted, unencrypted, or  
16 encrypted using a non-preferred encryption technique. As part of this step, as noted  
17 above, the digital content 111 is ultimately transformed into a format using a preferred  
18 encryption technique before being transferred to any devices other than the formatted-  
19 media reader 141c. As a result of this step, the local library 141 obtains at least a portion  
20 of the digital content 111 representing one or more media streams, and the method 200  
21 is able to proceed at the flow point 220.

1           At a flow point 220, the local library 141 is ready to partially decode the  
2 digital content 111. Steps following this flow point are optionally performed as part of  
3 the method 200.

4  
5           At a step 221, the local library 141 partially decodes the received digital  
6 content 111, with the effect of obtaining, in the clear, at least some metadata regarding  
7 that digital content 111. In one embodiment, the metadata obtained in the clear in-  
8 cludes at least one index file including pointers to selected locations within the media  
9 stream represented by the digital content 111. The method 200 is able to proceed at the  
10 flow point 230.

11  
12           At a flow point 230, the local library 141 is ready to maintain digital con-  
13 tent 111 in the memory or mass storage 141b.

14  
15           At a step 231, the local library 141 records the digital content 111 in the  
16 memory or mass storage 141b.

17  
18           At a step 232 (if the steps following the flow point 220 were performed),  
19 the local library 141 records any metadata obtained in response to the digital content  
20 111 in the memory or mass storage 141b.

1           As a result of performing the steps following the flow point 230, the local  
2 library 141 is able to retrieve the encrypted digital content 111, and optionally at least  
3 some unencrypted metadata associated therewith, from the memory or mass storage  
4 141b. The method 200 is able to proceed with the flow point 240.

5  
6           At a flow point 240, the local library 141 is ready to send the encrypted  
7 digital content 111 to the player equipment 143.

8  
9           At a step 241, the local library 141 retrieves the encrypted digital content  
10 111, and optionally at least some unencrypted metadata associated therewith, from the  
11 memory or mass storage 141b.

12  
13           At a step 242, the local library 141 sends that encrypted digital content 111  
14 from the memory or mass storage 141b, using the local network 142, to the player  
15 equipment 143.

16  
17           As a result of performing the steps following the flow point 240, the  
18 player equipment 143 is able to access the encrypted digital content 111. The method  
19 200 is able to proceed with the flow point 250.

20  
21           At a flow point 250, the player equipment 143 is ready to present the en-  
22 crypted digital content 111 to the user 150.

1  
2           At a step 251, the player equipment 143 receives the encrypted digital  
3 content 111, using the local network 142, from the memory or mass storage 141b.

4  
5           At a step 252, the player equipment 143 receives a set of commands or re-  
6 quests from the user 150.

7  
8           At a step 253, the player equipment 143 performs those commands or re-  
9 quests from the user 150 capable of being performed without reference to encrypted  
10 elements of the decoded digital content 111, without performing any decryption on that  
11 decoded digital content 111. As part of this step, the player equipment 143 might per-  
12 form one or more of the following sub-steps:

13  
14           At a sub-step 253a, the player equipment 143 might rewind, fast forward, or oth-  
15 erwise "seek" to a selected location within the digital content 111.

16  
17           At a sub-step 253b, the player equipment 143 might pause or halt presentation of  
18 the media stream represented by the digital content 111.

19  
20           At a step 254, the player equipment 143 performs those commands or re-  
21 quests from the user 150 to perform the media stream represented by the digital content  
22 111. To perform this step, the player equipment 143 performs the following sub-steps:

1  
2 At a sub-step 254a, the player equipment 143 decodes the digital content 111,  
3 with the effect of obtaining metadata describing presentation of the media  
4 stream, and encrypted data for presentation of the actual audio and video associ-  
5 ated with the media stream.

6  
7 At a sub-step 254b, the player equipment 143 sends encrypted digital content 111  
8 to a supplemental device (or a secure sub-system) for decryption.

9  
10 At a sub-step 254c, the player equipment 143 receives decrypted digital content  
11 111 from the supplemental device (or the secure sub-system) after decryption.

12  
13 At a sub-step 254d, the player equipment 143 presents the media stream in re-  
14 sponse to the decrypted digital content 111.

15  
16 At a flow point 260, the player equipment 143 is ready to respond to fur-  
17 ther commands from the user 150, and is able to proceed with the flow point 250.

18  
19 *Alternative Embodiments*

20  
21 The invention is useful for, and has sufficient generality for, applications  
22 other than distribution of media streams, and to other than distribution of digital con-

1 tent. For example, the invention is also generally useful for applications in which secu-  
2 rity of datasets or identifying recipients of those datasets is desired.

3  
4 Although preferred embodiments are disclosed herein, many variations  
5 are possible which remain within the concept, scope, and spirit of the invention. These  
6 variations would become clear to those skilled in the art after perusal of this applica-  
7 tion.

- 8
- 9 • As noted above, the invention is not restricted to movies, but is also applicable to  
10 other media streams, such as for example animation or sound, as well as to still  
11 media, such as for example pictures or illustrations, and to databases and other  
12 collections of information.

13  
14 Those skilled in the art will recognize, after perusal of this application,  
15 that these alternative embodiments are illustrative and in no way limiting.